Amendment to the Written Description

On page 7, lines 3-18, please replace the existing paragraph with the following substitute paragraph:

FIGURE 2 is a block diagram of a prior art system 30 for intrusion data collection. By way of example, the system 30 is a Transmission Control Protocol/Internet Protocol-compliant (TCP/IP) computing environment, such as described in W.R. Stevens, "TCP/IP Illustrated," Vol. 1, Ch. 1 et seq., Addison-Wesley (1994), the disclosure of which is incorporated herein by reference. However, the present discussion can equally be applied to other layered network architectures, including those based on the ISO/OSI model. A client 11 (shown in FIGURE 1) is physically interconnected to an intranetwork 13 (or internetwork 14) via a network interface controller (NIC) 31. Incoming data frames are processed through an internet protocol (IP) stack 33 for eventual delivery to host applications 40. Similarly, outgoing data packets originating from the host applications 40 are processed through the IP stack 33 for eventual transmission over the intranetwork 13. A C2 auditing system 34 provides host-based security by monitoring system-level activities. A host collector 35 receives the monitoring data which is reported to an analysis module 36 for intrusion analysis and detection.

On page 8, lines 7-16, please replace the existing paragraph with the following substitute paragraph:

As a hardware device, the NIC [[~~33~~]] 31 is outside the kernel memory space 32 but the actual copying of the network traffic from the NIC [[~~33~~]] 31 to the packet filter 37 is performed by a network driver (not shown) also operating in the kernel memory space 32. Consequently, the copying of each data frame is computationally expensive due to the context switch and sheer volume of data copied. Similarly, the demultiplexing of raw data by the stream and packet processing module 38 duplicates the work performed by the IP stack 33 and

introduces the potential for erroneously reassembled packets. These shortcomings can be exploited by a would-be network intruder and introduces problems when trying to accurately detect certain types of attacks.